ADA Mobile Profile
Letter of Assessment (LOA) for: LastPass - Password Manager

LastPass
Version 1.0 – Nov 17, 2025

Prepared By
Thomas Cannon
Victor Lasa

Prepared For
Pedro Correia

1 ADA Mobile Profile Letter of Assessment

In September and October of 2025, NCC Group performed an App Defense Alliance (ADA) Mobile Profile Assessment against Password Manager v6.35.1.17426 (the "**Application**") for and on behalf of LastPass ("**Developer**") pursuant to the governing contract(s) between NCC Group and Developer. The assessment objective was to identify compliance with the ADA Mobile Profile framework within a time-boxed assessment. ADA Mobile Profile is defined by the App Defense Alliance (ADA) and is based on the OWASP Mobile Application Security Verification Standard (MASVS). For more specific information on the specific requirements assessed, please see Appendix A.

This Letter of Assessment ("**LOA**") confirms that the assessment of the Application has been completed and was found to substantially comply with the requirements in Appendix A.

It is important to note that this LOA represents a point-in-time evaluation. The security and compliance of an application can evolve rapidly, and the results of this assessment are not intended to represent an endorsement of the Application's future compliance or adequacy of current security measures against future threats. This LOA necessarily contains information in summary form and is therefore intended for general guidance only; it is not intended as a substitute for detailed research or the exercise of professional judgment. The information presented here should not be construed as professional advice or service.

Technical Constraints

The following items may impact the completeness and accuracy of the test case results:

- The ADA Mobile Profile framework was in active development during the assessment. Some controls may have been modified during or after the testing period.
- Some controls employed ambiguous language. When presented with equally valid interpretations of a control, NCC Group selected the strictest version unless otherwise directed by Google.

Terms, Limitations and Disclaimers

- Prepared by NCC Group Security Services, Inc. for Developer.
- Portions of this document and the templates used in its production are the property of NCC Group and cannot be copied or disclosed (in full or in part) without NCC Group's prior written permission.
- While precautions have been taken in the preparation of this document, NCC Group the publisher, and the author(s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein.
- NCC Group provides no warranty or guarantee that any of NCC Group's services including but not limited to, recommendations, results or assessments will prevent or avoid any future security breaches or unauthorized access to the Application or Developer's networks or systems.
- ADA Mobile Profile is intended to provide more transparency into application security, however the limited nature of testing does not guarantee complete safety of the Application. This independent review may not be scoped to verify the accuracy and completeness of a developer's data safety declarations. Developer remains solely responsible for making complete and accurate declarations in their app's Google listings.
- NCC Group further expressly disclaims all warranties and conditions of any kind, whether express or implied, including, but not limited to the implied warranties and conditions of merchantability, fitness for a particular purpose and non-infringement.

APPENDIX A: ADA Mobile Profile Requirements as Tested

Requirements used for this LOA are outlined below. These are based on ADA Mobile Profile version 1.0 dated 10/10/2024 per the Application Defense Alliance Mobile App Test Guide (ADAMATG). Where there are differences between below requirements and ADAMATG, the below requirements were followed.

The "MSTG-ID" column refers to the related OWASP Mobile Application Security Testing Guide (MASTG, previously known as Mobile Security Testing Guide, MSTG) requirements upon which the listed ADA Mobile Profile requirement is based.

Legend:

- **PASS** = NCC Group did not observe significant non-compliance with the indicated ADA Mobile Profile Requirements during testing.
- **FAIL** = NCC Group observed significant non-compliance with the indicated Requirement during testing.
- **INC** = "Inconclusive," NCC Group was unable to verify compliance with the indicated Requirement either due to ambiguity in observed evidence or of the Requirement itself. This is effectively a FAIL from an overall LOA standpoint.
- **NA** = "Not Applicable," NCC Group judged the Requirement to be inapplicable to the target application. This is effectively a PASS from an overall LOA standpoint.

ID	MSTG-ID	Description	Status
1.1 Storage			
1.1.1.1	MASTG-TEST-0001	The app shall securely store sensitive data in external storage	Pass
1.1.2.1	MASTG-TEST-0006	The Keyboard Cache Is Disabled for sensitive data inputs	Pass
1.1.2.2	MASTG-TEST-0003	No sensitive data is written to application logs.	Pass
1.2 Crypto			
1.2.1.1	MASTG-TEST-0016	No insecure random number generators shall be utilized for any security sensitive context	Pass
1.2.1.2	MASTG-TEST-0013	No insecure operations shall be used for symmetric cryptography	Pass
1.2.1.3	MASTG-TEST-0014	Strong cryptography shall be implemented according to industry best practices	Pass
1.2.2.1	MASTG-TEST-0015	Cryptographic keys shall only be used for their defined purpose	Pass
1.2.2.2	MASTG-TEST-0062	Cryptographic key management shall be implemented properly	Pass
1.3 Auth			
1.3.1.1	N/A	If using OAuth 2.0 for authorization, or if using OpenID Connect for authentication, Proof Key for Code Exchange (PKCE) shall be implemented to protect the code grant	Pass
1.4 Network			

ID	MSTG-ID	Description	Status
1.4.1.1	MASTG-TEST-0019	Network connections shall be encrypted	Pass
1.4.1.2	MASTG-TEST-0020	TLS configuration of network connections shall adhere to industry best practices	Pass
1.4.1.3	MASTG-TEST-0021	Endpoint identity shall be verified on network connections	Pass
1.5 Platform			
1.5.1.1	MASTG-TEST-0007	The app shall limit content provider exposure and harden queries against injection attacks	Pass
1.5.1.2	MASTG-TEST-0028	The app shall use verified links and sanitize all link input data	Pass
1.5.1.3	MASTG-TEST-0029	Any sensitive functionality exposed via IPC shall be intentional and at the minimum required level	Pass
1.5.1.4	MASTG-TEST-0030	All Pending Intents shall be immutable or otherwise justified for mutability	Pass
1.5.2.1	MASTG-TEST-0031	WebViews shall securely execute JavaScript	Pass
1.5.2.2	MASTG-TEST-0032	WebView shall be configured to allow the minimum set of protocol handlers required while disabling potentially dangerous handlers	Pass
1.5.3.1	MASTG-TEST-0008	The app shall by default mask data in the User Interface when it is known to be sensitive	Pass
1.6 Code			
1.6.1.1	N/A	The app shall set the targetSdkVersion to an up-to-date platform version	Pass
1.6.2.1	MASTG-TEST-0042	The app only uses software components without known vulnerabilities	Pass
1.6.3.1	MASTG-TEST-0044	Compiler security features shall be enabled	Pass
1.6.3.2	MASTG-TEST-0025	The App shall Mitigate Against Injection Flaws in Content Providers	Pass
1.6.3.3	MASTG-TEST-0027	Arbitrary URL redirects shall not be included in the app's webviews	Pass
1.6.3.4	MASTG-TEST-0026	Any use of implicit intents shall be appropriate for the app's functionality and any return data shall be handled securely	Pass
1.7 Resilience			
1.7.1.1	MASTG-TEST-0038	The app shall be properly signed	Pass
1.7.2.1	MASTG-TEST-0040	The app shall disable all debugging symbols in the production version	Pass

ID	MSTG-ID	Description	Status
1.7.3.1	MASTG-TEST-0039	The app shall not be debuggable if installed from outside of commercial app stores	Pass
1.8 Privacy			
1.8.1.1	N/A	The app shall minimize access to sensitive data and resources provided by the platform	Pass
1.8.2.1	N/A	The app shall be transparent about data collection and usage	Pass
1.8.3.1	N/A	Users shall have the ability to request their data to be deleted via an in-app mechanism	Pass